



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

09/143,907 08/31/98 CARLSON

R 1505/5

EXAMINER

TM02/0619

ROBERT C DORR
DORR CARSON SLOAN & BIRNEY
3010 E 6TH AVENUE
DENVER CO 80206

MAIL
ART UNIT

PAPER NUMBER

2121
DATE MAILED:

06/19/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.

09/143,907

Applicant(s)

Examiner

Mai, T.

Group Art Unit

2121

—The MAILING DATE of this communication appears on the cover sheet beneath the correspondence address—

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, such period shall, by default, expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

- ☒ Responsive to communication(s) filed on 5-7-01
- ☐ This action is **FINAL**.
- ☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

- ☒ Claim(s) 26-27, 29-46 is/are pending in the application.
- Of the above claim(s) 29-46 is/are withdrawn from consideration.
- ☐ Claim(s) _____ is/are allowed.
- ☒ Claim(s) 26-27 is/are rejected.
- ☐ Claim(s) _____ is/are objected to.
- ☐ Claim(s) _____ are subject to restriction or election requirement.

Application Papers

- ☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.
- ☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.
- ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.
- ☐ The specification is objected to by the Examiner.
- ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119 (a)-(d)

- ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).
 - ☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been received.
 - ☐ received in Application No. (Series Code/Serial Number) _____
 - ☐ received in this national stage application from the International Bureau (PCT Rule 1.7.2(a)).

*Certified copies not received: _____

Attachment(s)

- ☒ Information Disclosure Statement(s), PTO-1449, Paper No(s) 3
- ☒ Notice of Reference(s) Cited, PTO-892
- ☒ Notice of Draftsperson's Patent Drawing Review, PTO-948
- ☐ Interview Summary, PTO-413
- ☐ Notice of Informal Patent Application, PTO-152
- ☐ Other _____

Office Action Summary

Art Unit: 2121

1. Applicant's election without traverse of Group I, Claims 26-27, in Paper No. 8 is acknowledged.

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 26-27 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for a method for generating random numbers as shown and detailed in Fig. 7, does not reasonably provide enablement for a method for generating random numbers having **encrypting** feature. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these claims. It is noted that the specification has merely mentioned about the **encrypting**; however, the flowchart of Fig. 7 does not detailed the feature.

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aiello et al'307 in view of Aiello et al'928.

Art Unit: 2121

As per independent claim 26, Aiello et al'307 shows, see Fig. 1, a pseudo-random generator substantially as claimed. For example, Col. 3, lines 25-34, "a method for generating *an output stream of cryptographically strong pseudo-random bits from an input stream ... The input stream is then utilized to form a seed ... Next, a set of bits is selected ...*" are considered claimed **providing, encrypting and grouping steps**. It is noted that Aiello et al'307 do not show the claimed (1) **continuously changing deterministic output** and (2) **verifying step**. First, Aiello et al'928 show another pseudo-random generator having **timing feature** (e.g., see Fig. 3) for continuously function. Second, Aiello et al'307 show the equivalent **verifying feature**, e.g. see Col. 3, lines 54-56, "[o]n the otherhand, P₀'s **outputs are almost k-wise independent: ...**". Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to combine Aiello et al'928 in Aiello et al'307 because the proposed device has the claimed features.

As per dependent claim 27, the claimed **storing and distributing steps** are obvious to a person having ordinary skill in the art. For example, the Aiello et al's systems could have memory for storing the processed data. The processors (230, 240) have different sizes of outputs. Therefore, a portion of process data has been distributed by one of the processor.

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Cited references are art of interest.

Art Unit: 2121

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tan V. Mai whose telephone number is (703) 305-9761. The examiner can normally be reached on Tue-Fri from 6:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William A. Grant, can be reached on (703) 308-1108. The fax phone number for the organization where this application or proceeding is assigned is (703) 306-5404.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3800

TM.



TAN V. MAI
PRIMARY EXAMINER